

MDA Software Assurance (SwA) Approach



To: 2018 MDA Small Business Programs Conference

**By: Dr. Michael Wojcik
DA Information System Security Manager
Michael.Wojcik@mda.mil
Missile Defense Agency
May 15, 2018**

Approved for Public Release
18-MDA-9632 (10 May 18)



Agenda

- Introduction**
- MDA SwA Approach**
 - **Build In Software Security**
 - **Assess Software Security**
 - **Manage Software Security Risk**
- Summary**



Introduction

What is Software Assurance and why do we need it?



Software Assurance is... the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.¹

**Public Law
112-239**

Public Law 112-239 mandates that software assurance be included for MDA trusted defense systems.

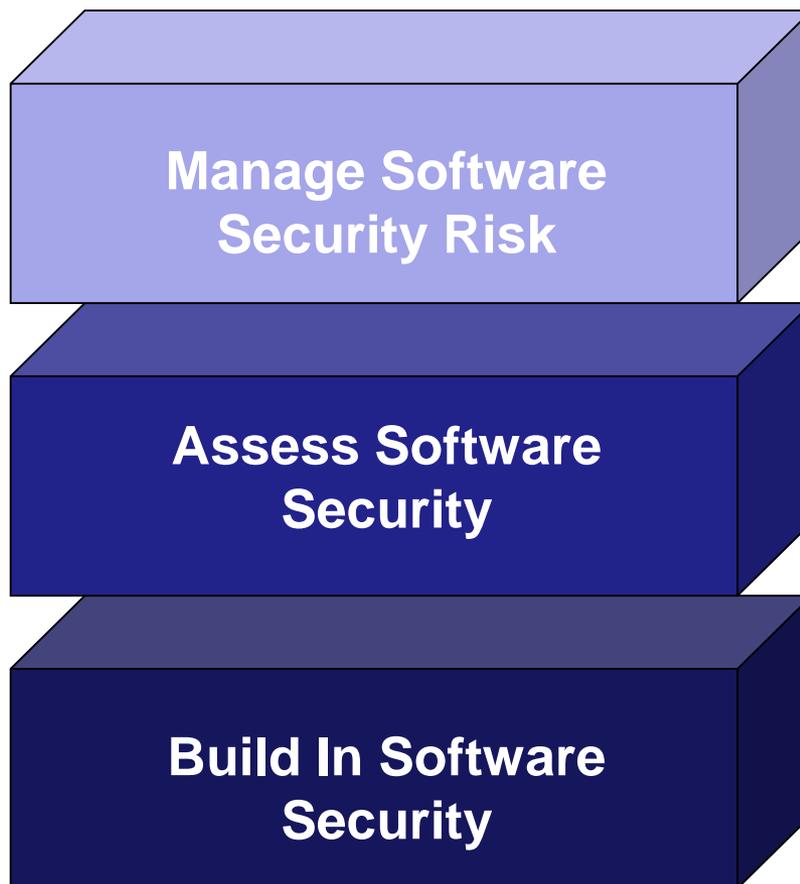
¹ DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)", Change 1, August 25, 2016, Page 13



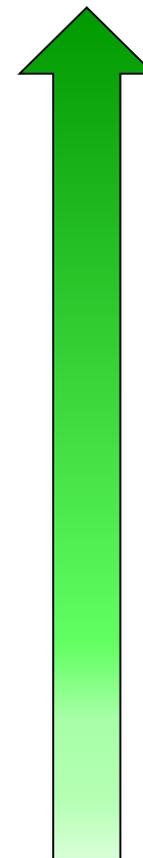
MDA SwA Approach

SwA Activities

- Assess, mitigate, and manage SwA risk
- Independent SwA Assessment
- SwA requirements on contract and developer practices verified

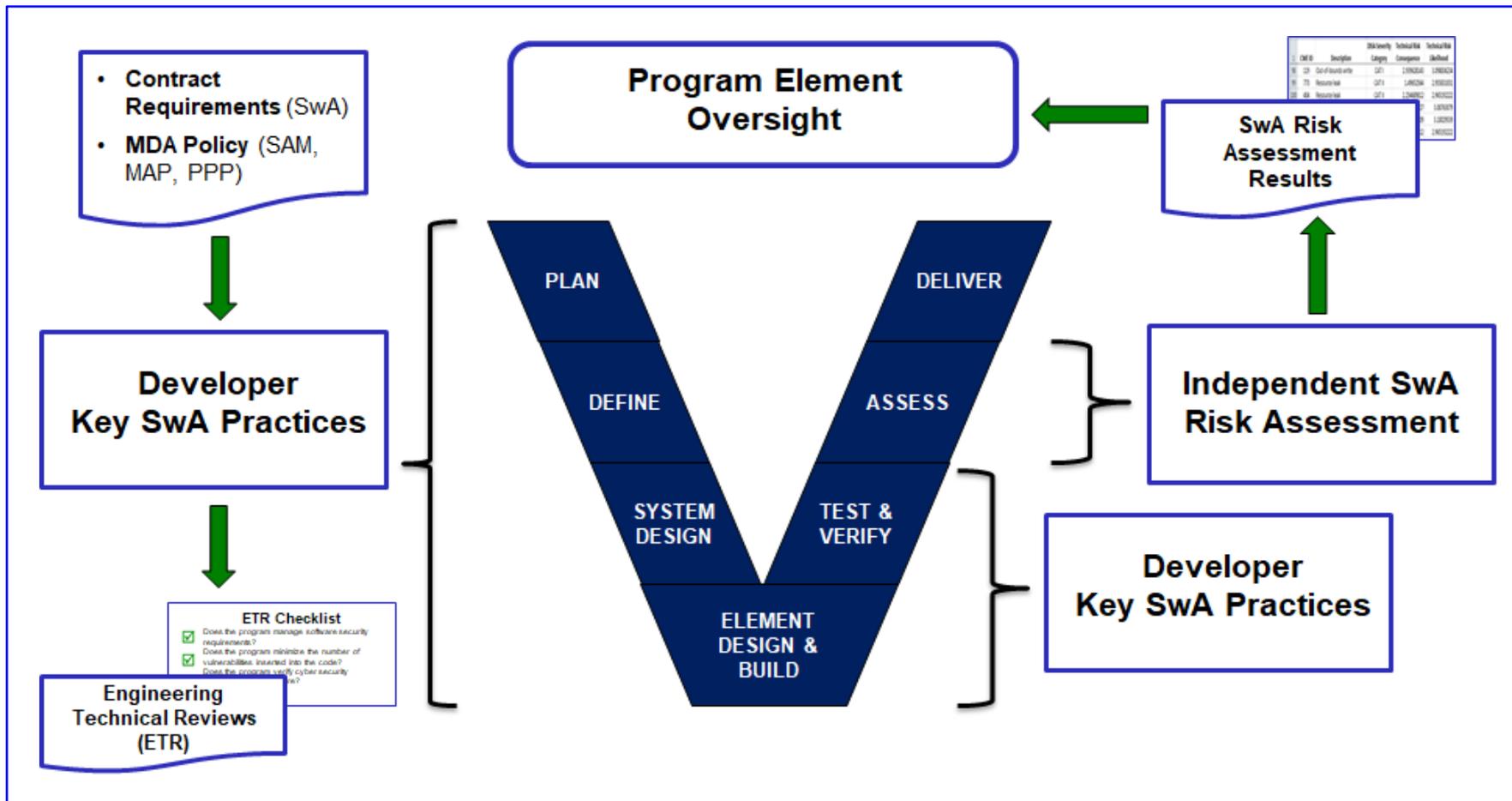


SwA
Confidence





SwA and the Systems Engineering Process





Build In Software Security

Program Element SwA activities:

1. Build In Software Security

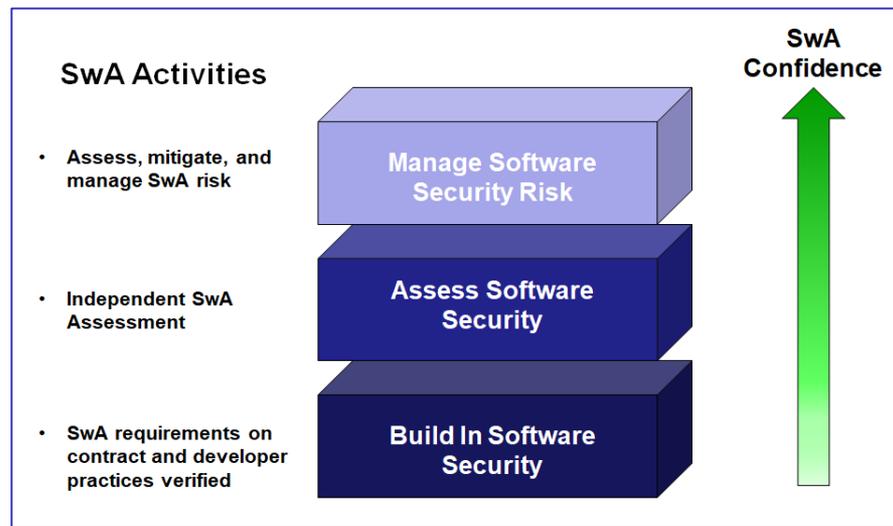
- Ensure SwA requirements are placed on contract
- Verify developer key SwA practices at ETR milestone reviews

2. Assess Software Security

- Incorporate an independent SwA assessment into software IV&V activities

3. Manage Software Security Risk

- Assess and mitigate SwA risk identified throughout the software lifecycle
- Manage SwA risk in accordance with MDA instructions





MDA SwA Requirements

MDA RMF SwA Overlay:

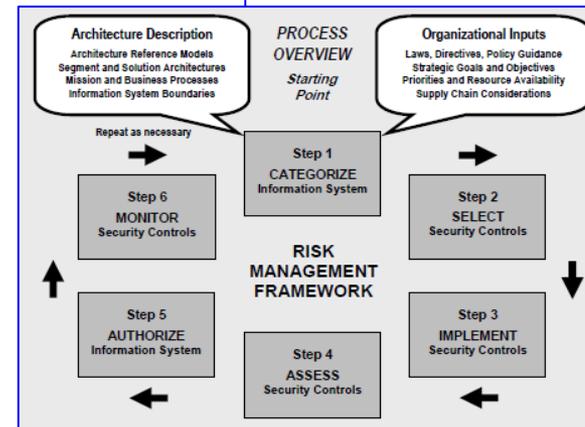
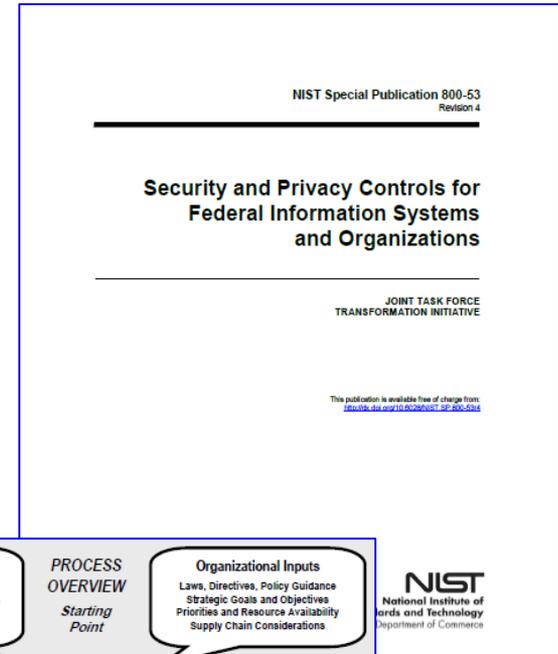
- The MDA RMF SwA Overlay defines specific SwA requirements that are to be applied to MDA Systems based upon system type:
 - **Tactical Mission System** - A system that is integrated into the BMDS and is included as a part of the BMDS Operational Capacity Baseline (OCB).
 - **Mission Support System** – A system that supports the development, testing, evaluation, or monitoring of BMDS Tactical Mission System components.
 - **Enterprise Support System** – A system that provides general administrative support for Missile Defense Agency (MDA) business operations, collaboration, or communication.



MDA SwA Requirements

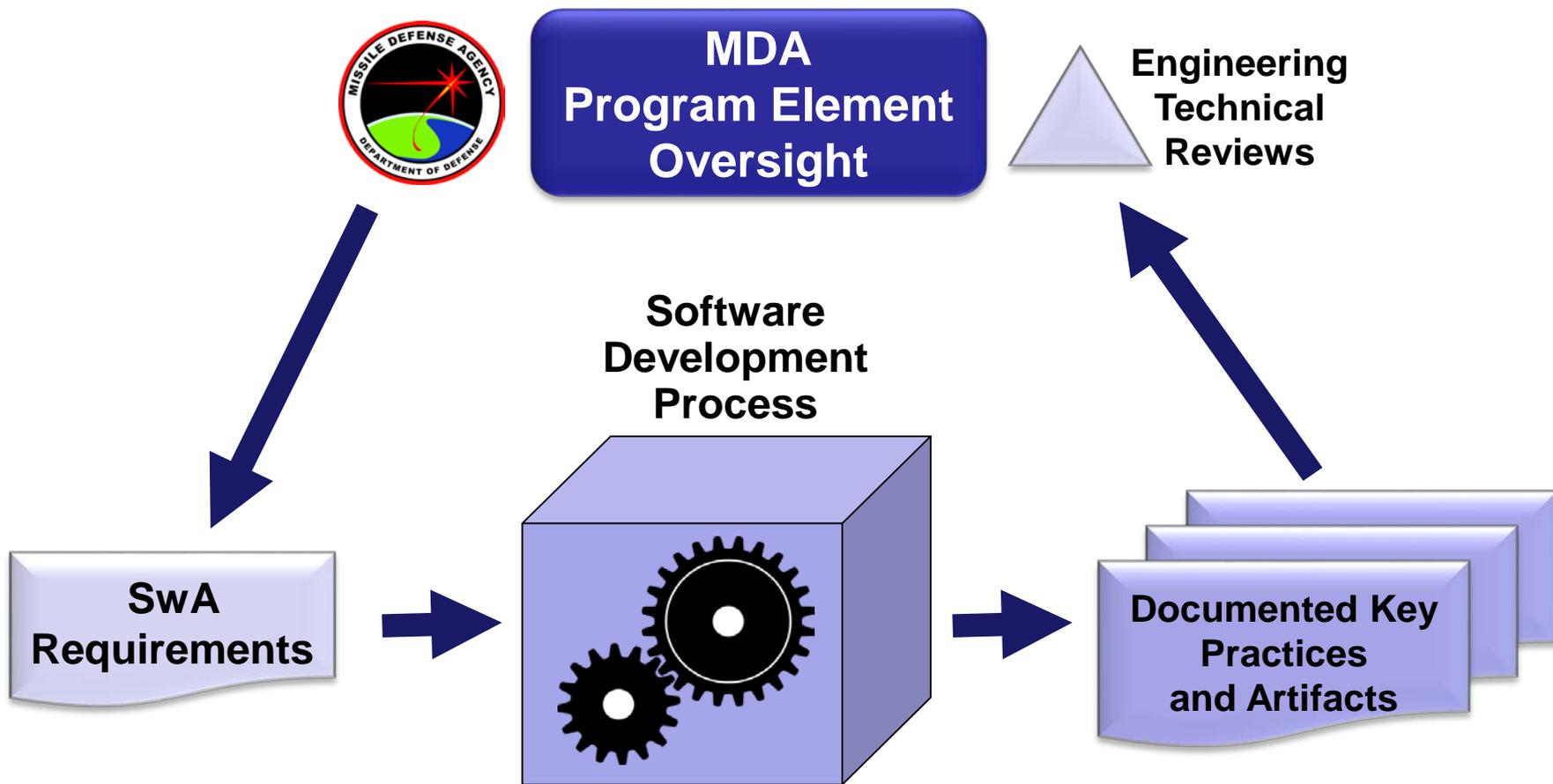
MDA SwA Requirements:

- Program Executives will **plan and budget** for inclusion of requirements specified in the “MDA Software Assurance Overlay” on all contracts and ensure these requirements are incorporated into the statement of work (SOW), as part of the Contract Requirements Package (CRP).
- SwA requirements will be **identified and selected** during Steps 1 and 2 (CATEGORIZE Information System and SELECT Security Controls”) steps of the RMF process.





Evaluating SwA Key Practices



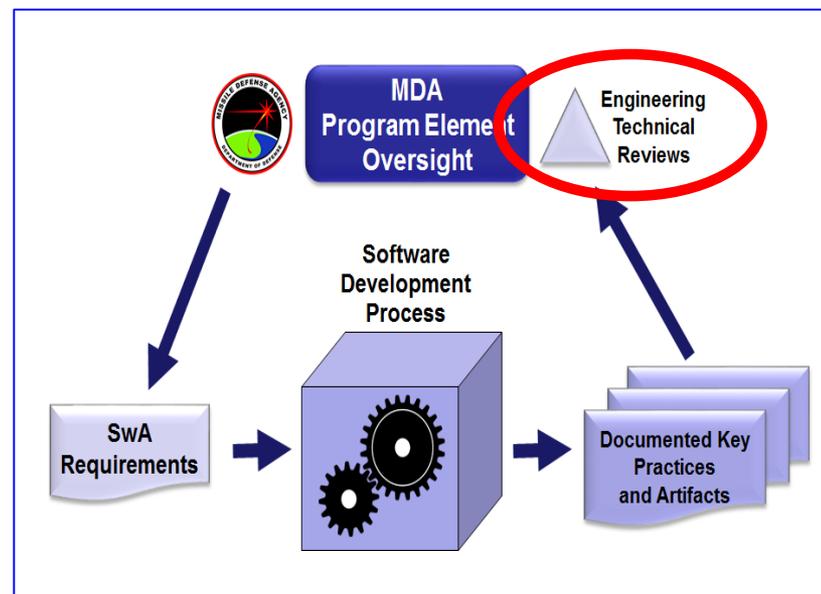


Engineering Technical Reviews

❑ MDA Instruction 5000.20-INS

SwA entrance and exit criteria have been added to MDA's Engineering Technical Review Process:

- SwA Entrance and Exit Criteria Added
 - System Requirements Review (SRR)
 - Preliminary Design Review (PDR)
 - Critical Design Review (CDR)
 - Test Readiness Review (TRR)

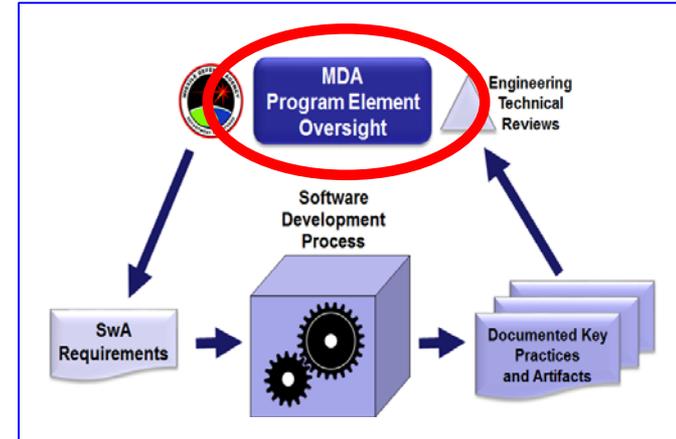




Program Element Oversight

❑ Program Element Oversight

- Standard CDRLs
 - SRS, SDD SDP, CMP, STP, etc.
- SwA-specific CDRLs
 - Software Assurance Evaluation Report
 - Software Attack Surface Analysis Report
 - Vulnerability Assessment Report
 - Software Threat Analysis Report
- ✓ SwA-specific CDRLs submitted to the Government for each final software release.
- ✓ A current report delivered 30 days prior to each major technical review.
- ✓ Contractor's working products made available for review at other times by the Government upon request.





Independent SwA Assessment

Program Element SwA activities:

1. Build In Software Security

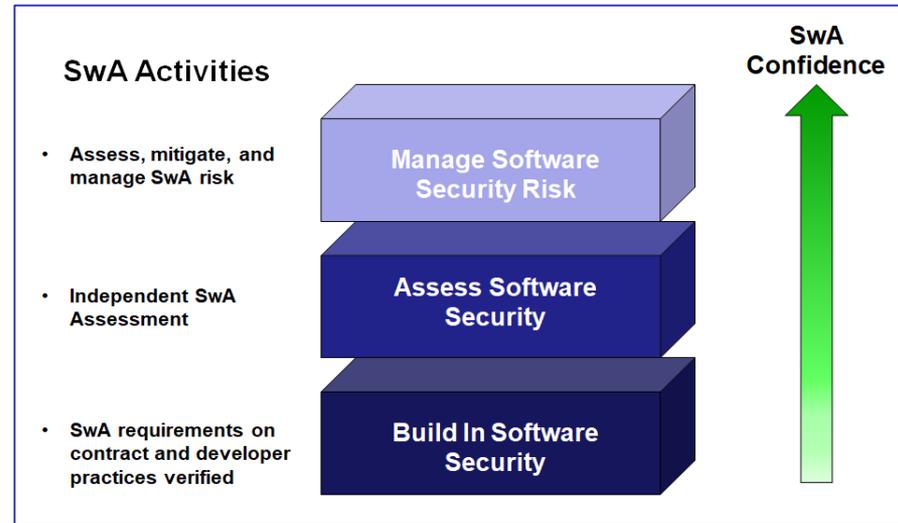
- Ensure SwA requirements are placed on contract
- Verify developer key SwA practices at ETR milestone reviews

2. Assess Software Security

- Incorporate an independent SwA assessment into software IV&V activities

3. Manage Software Security Risk

- Assess and mitigate SwA risk identified throughout the software lifecycle
- Manage SwA risk in accordance with MDA instructions

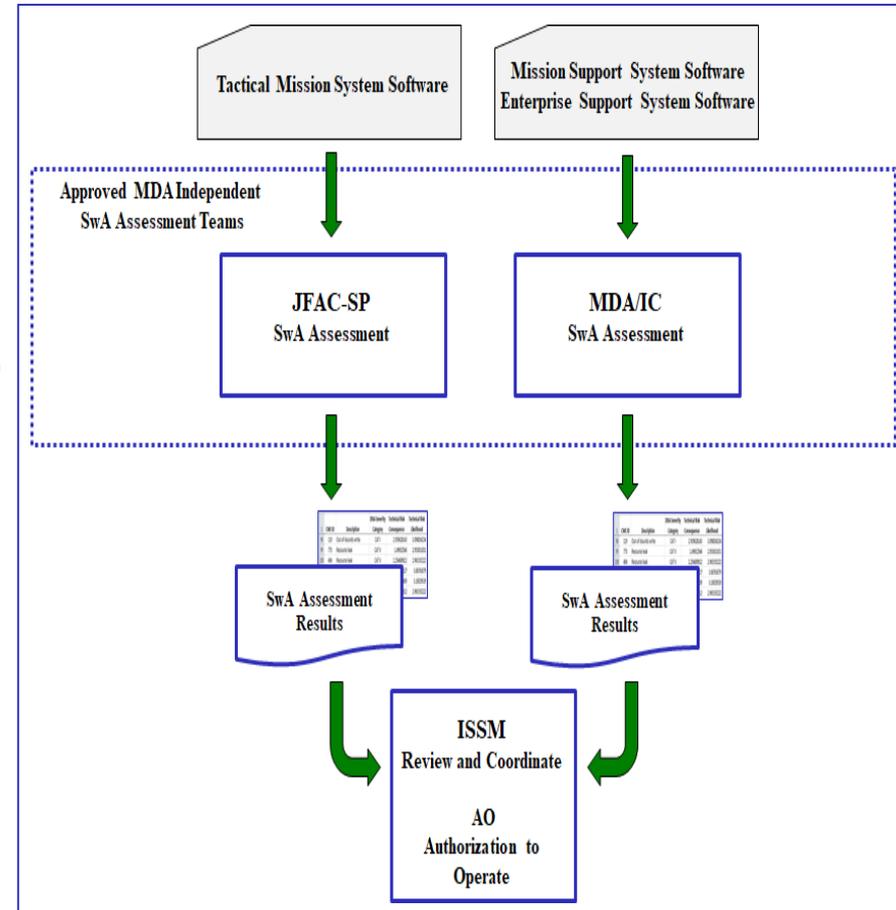




Independent SwA Assessment Teams

SwA Assessment Teams:

- **JFAC Service Providers**
 - Primary responsibility for assessing:
 - **BMDS Tactical Mission System software** (i.e., software that is included as a part of the BMDS Operational Capacity Baseline (OCB))
- **MDA/IC**
 - Primary responsibility for assessing:
 - **Mission Support System software** (i.e., software that supports the development, testing, evaluation, or monitoring of BMDS Tactical Mission System components)
 - **Enterprise Support System software** (i.e., software that provides general administrative support for MDA business operations, collaboration, or communication.)





Manage Software Security Risk

Program Element SwA activities:

1. Build In Software Security

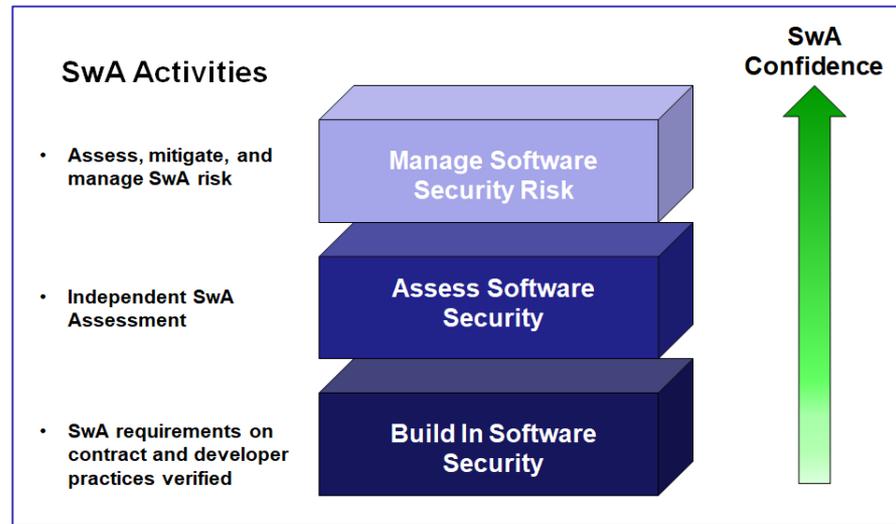
- Ensure SwA requirements are placed on contract
- Verify developer key SwA practices at ETR milestone reviews

2. Assess Software Security

- Incorporate an independent SwA assessment into software IV&V activities

3. Manage Software Security Risk

- Assess and mitigate SwA risk identified throughout the software lifecycle
- Manage SwA risk in accordance with MDA instructions

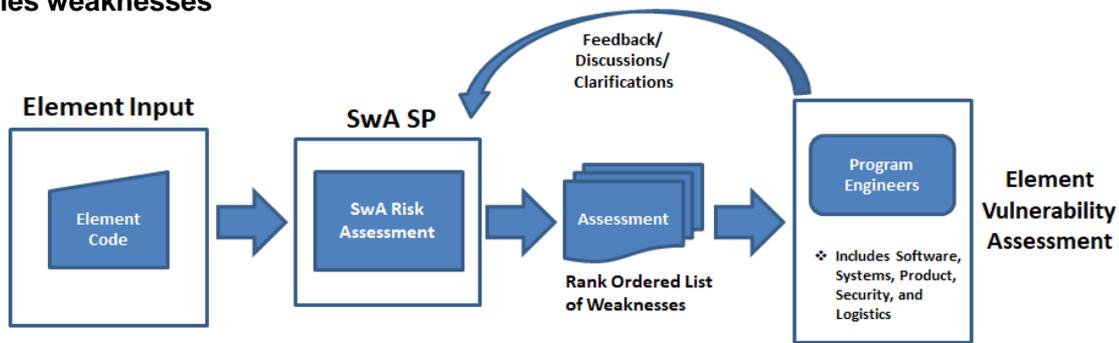




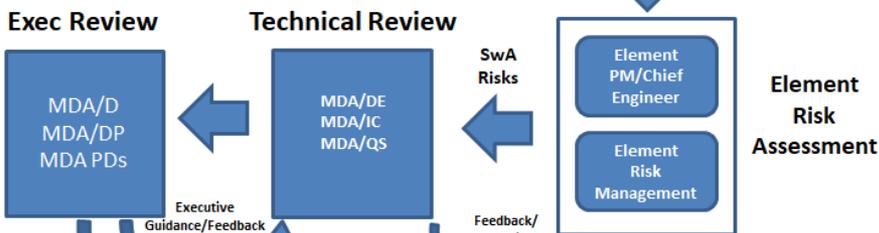
SwA Risk Assessment Process Flow

Step 1: SwA SP assesses software and identifies weaknesses

Software Weakness – a deficiency, flaw, defect, or limitation in code, design, or architecture that can lead to a software vulnerability



Step 2: Element reviews SwA weaknesses and mitigating controls to determine vulnerabilities



Step 3: Element addresses and corrects SwA vulnerabilities

Step 5: SwA risks are reported to and managed by MDA Executives

- Assess Risk
 - Recommendations to Acceptance Authority
- Executive Guidance/Feedback (Risk Owner)
- SwA Risks Identified
 - Likelihood Quantified
 - Consequence Defined
 - Mitigation Determined
 - Dependencies Identified
- Feedback/corrections

Step 4: Element documents residual SwA risks and mitigation plans

Software Vulnerability – a weakness in software that may be exploited, resulting in a negative impact to confidentiality, integrity, or availability



Summary

- **MDA SwA Goal:** to improve the integrity of MDA software and minimize risk, by identifying and mitigating software vulnerabilities before fielding

- **MDA SwA Approach:**
 - Build in Software Security
 - Assess Software Security
 - Manage Software Security Risk

